Process Based Mission Assurance SecureMeeting Procedures

Prepared for the
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
Report No. 0190602.17.001

August 24, 2004

ARES CORPORATION
21000 Brookpark Road
MS 501-4
Cleveland, OH 44135

TABLE OF CONTENTS

1 Introduction

Process Based Mission Assurance (PBMA) SecureMeeting is a collaboration tool that allows users to securely schedule and hold online meetings that involve Administratively Controlled Information (ACI) data. In meetings, users can share their complete desktops or individual applications over a 128-bit encrypted, secure connection. SecureMeeting attendees can also remote-control one another's desktops and chat using a separate application window that does not interfere with the presentation.

The only function of this system is to permit users to collaborate and display sensitive data through a secure meeting functionality. This is a “virtual sharing” of visual information, which means no files are transmitted. Therefore, the system is no more than a pass-through for information to be shared via secure online meetings and does not retain any of the meeting data. This system is designed specifically for the sharing of ACI data through display only. This system is **not** certified nor accredited to handle or display classified national security information. Any sharing beyond specifically authorized individuals with a determined “need-to-know” is in violation of NASA Policy and may be in violation of Federal law.

Proper safeguarding is the responsibility of the individual in possession of ACI material to protect it from access by, or disclosure to, unauthorized persons. This means that it is incumbent upon each SecureMeeting account holder to protect the meetings in which they are conducting or attending.

2 Security Practices

All individuals who partake in secure meetings must take responsibility for protecting Administratively Controlled Information (ACI). ACI information must be safeguarded by protecting login information and restricting meeting access to only those who posses a need-to-know for the sensitive information being presented.

2.1 Administratively Controlled Information

Administratively Controlled Information is official information and material, of a sensitive but unclassified nature, which does not contain national security information (and therefore cannot be classified), nonetheless, should still be protected against inappropriate disclosure. Within NASA, such information may have previously been designated "FOR OFFICIAL USE ONLY." This NASA designation has been changed to "Administratively Controlled Information," for clarity and to more accurately describe the status of information to be protected.

2.2 Protecting Login Information

PBMA SecureMeeting accounts are granted only to individuals that have a need for meeting capability and are working on official NASA business. Access to the meeting application through login page uses a combination of user name and password.

Passwords are simpler and cheaper than other, more secure forms of authentication such as special key cards, fingerprint ID machines, and retinal scanners. They provide a simple, direct means of protecting a system or account. Being simpler and cheaper, they require greater attention by the user to protect. The following rules will be employed in the using of this system:

- Never record login information in an unprotected location - electronic or physical, where unauthorized individuals can access it.
- Passwords must be a minimum of eight characters. The eight characters will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, and special characters.
- Passwords must be changed every 90 days.

2.3 Meeting Monitoring

2.3.1 Meeting Security

Individuals with PBMA SecureMeeting accounts are responsible for ensuring that meeting attendance is limited to individuals with a legitimate need-to-know for the sensitive information being shared. Good security practices include:

- Always attending the system when in use.

- Ensuring that the system is inaccessible by unauthorized individuals, if it is necessary to step away from the system for any reason during the meeting,.
- Verifying that all attendees are eligible to have access to the information being presented in the meeting. If the meeting scheduler is not the Data Owner, check with the Data Owner to make sure that appropriate checks on meeting invitees have been conducted so that no unauthorized disclosures of the sensitive data occurs.
- Canceling meetings and notifying meeting invitees of cancellations.
- Removing meeting attendees as data is presented in which they do not have a need-to-know.
- Request SecureMeeting account deactivation when no longer needed.

2.3.2 Information

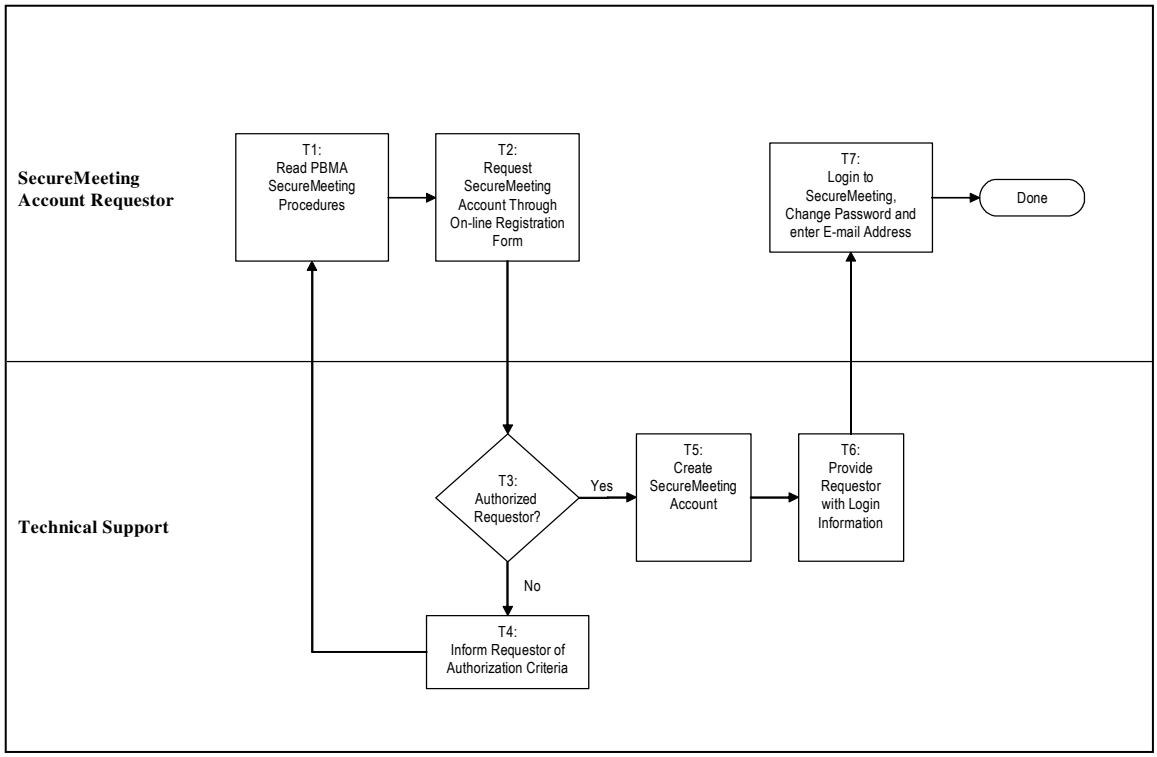
Individuals scheduling meetings should know the material to be shared and displayed at their meeting. **It is imperative that sensitive data is protected at all times.** Criteria of at least one of the following must be met to qualify as ACI:

- Information Protected by Statute: Export Administration Act; Arms Export Control Act; Space Act (Section 303b):
    - ITAR: International Traffic in Arms Regulations
    - EAR: Export Administration Regulations
    - MCTL: Military Critical Technologies List
    - FAR: Federal Acquisition Regulations
    - FOIA: Freedom of Information Act and the Privacy Act of 1996
    - UCNI: Unclassified Controlled Nuclear Information.
- Information the data owner determines to be unusually sensitive or critical to the success of the program or project
- Information Exempt from Freedom of Information Act (FOIA); which includes:
    - Internal Personnel Rules/Practices
    - Trade Secrets/Commercial/Financial
    - Inter/Intra-Agency Memos and Letters
    - Personnel and Medical Files
    - Investigative Records
    - Financial Institution Information
    - Geological/Geophysical
    - Maps/Documents of underground utilities
    - Drawings/specifications for Mission Essential Infrastructure (MEI) or other assets
    - Mission specific security plans
    - Emergency contingency plans

3 Process for Attaining a PBMA SecureMeeting Account

In order to setup and schedule meetings you must have a SecureMeeting account. **You must have a SecureMeeting account to attend meetings.** The following outlines the process for obtaining a SecureMeeting account:

Attaining a PBMA SecureMeeting Account



TASKS

T1. *Read the PBMA SecureMeeting Procedures:* Any individual requesting a SecureMeeting account must read the *PBMA SecureMeeting Procedures* to become familiar with the purpose of the application and the responsibilities associated with it.

T2. *Request SecureMeeting Account Through On-line Registration Form:* Request a SecureMeeting account through the PBMA-KMS Web site on-line registration form (http://pbma.nasa.gov/meeting/).

T3. *Authorized Requestor?:* Determine if the Requestor is authorized to request a SecureMeeting account.

T4. *Inform Requestor of Authorization Criteria:* If the requestor is not authorized to have a SecureMeeting account, refer them back to the *PBMA SecureMeeting Procedures* for an explanation of authorization criteria.

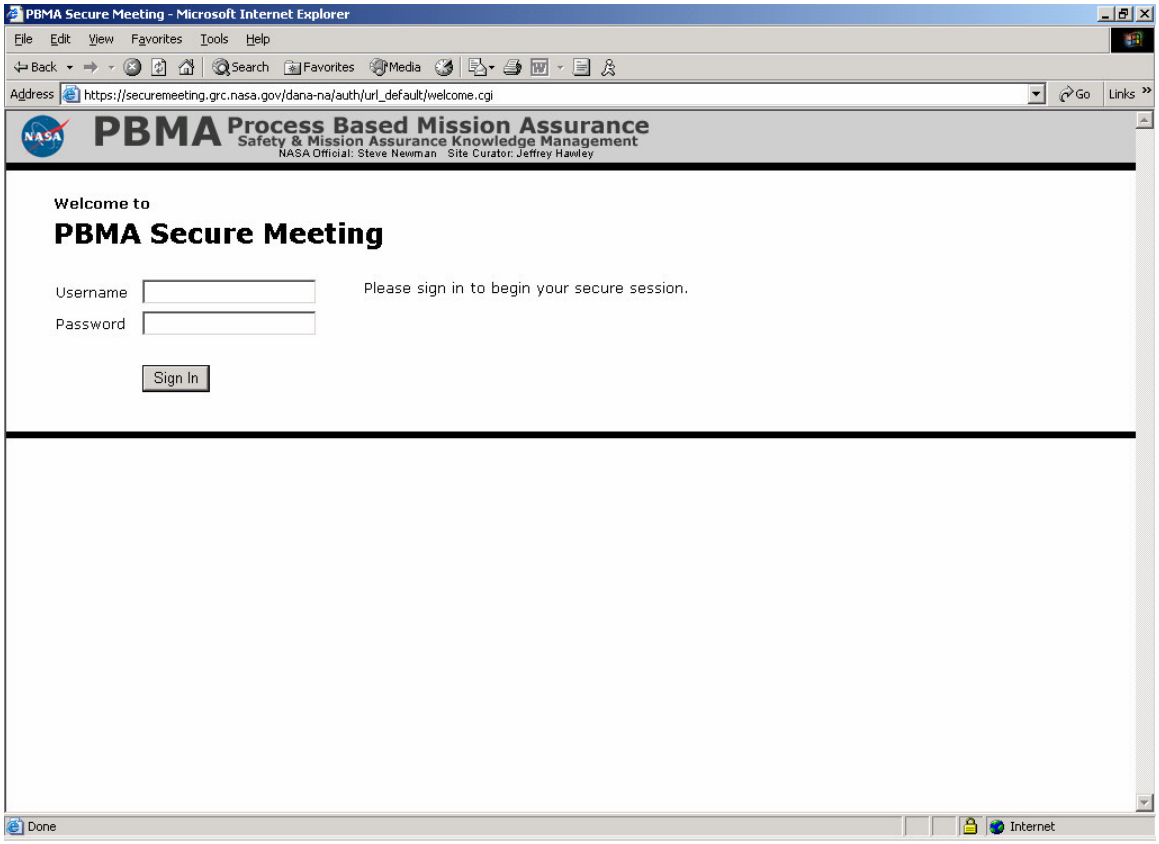
T5. *Create SecureMeeting Account:* Technical Support will create the requestor's SecureMeeting account

T6. *Provide Requestor with Login Information:* Technical Support then provides the requestor with their user name and initial password by telephone.

T7. *Login to SecureMeeting, Change Password and enter Email Address:* Requestor logs into the site and changes their password. Each user must change their password through the following steps:

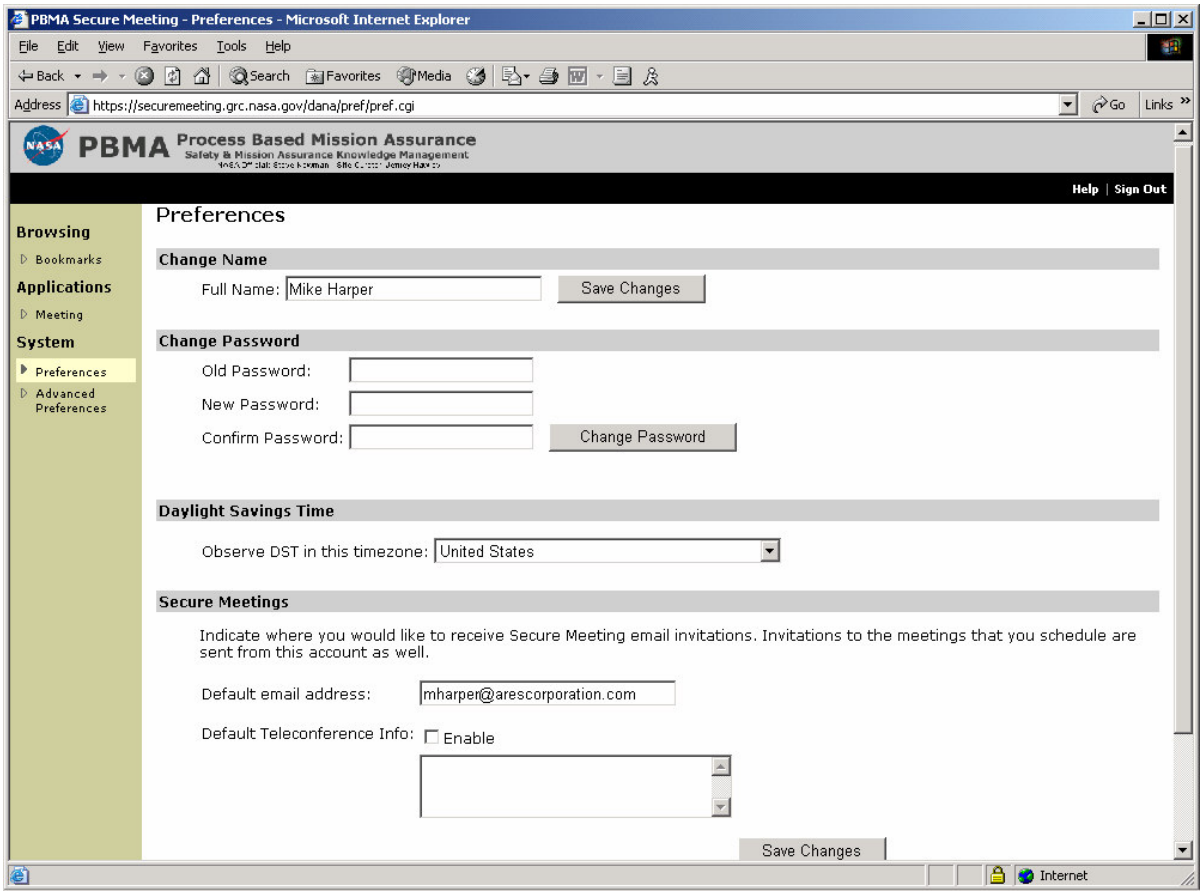
Step 1. Login through the SecureMeeting Login Page located at https://securemeeting.grc.nasa.gov

Login to SecureMeeting Account



Step 2. Go to the “Preferences” link

Preference Page



Step 3. Change your password from the one that was given to you by PBMA Technical Support.

Step 4. Enter in your email address.

Note: If you have a dedicated teleconference number, you can enter that information the “Default Teleconference Info” box.

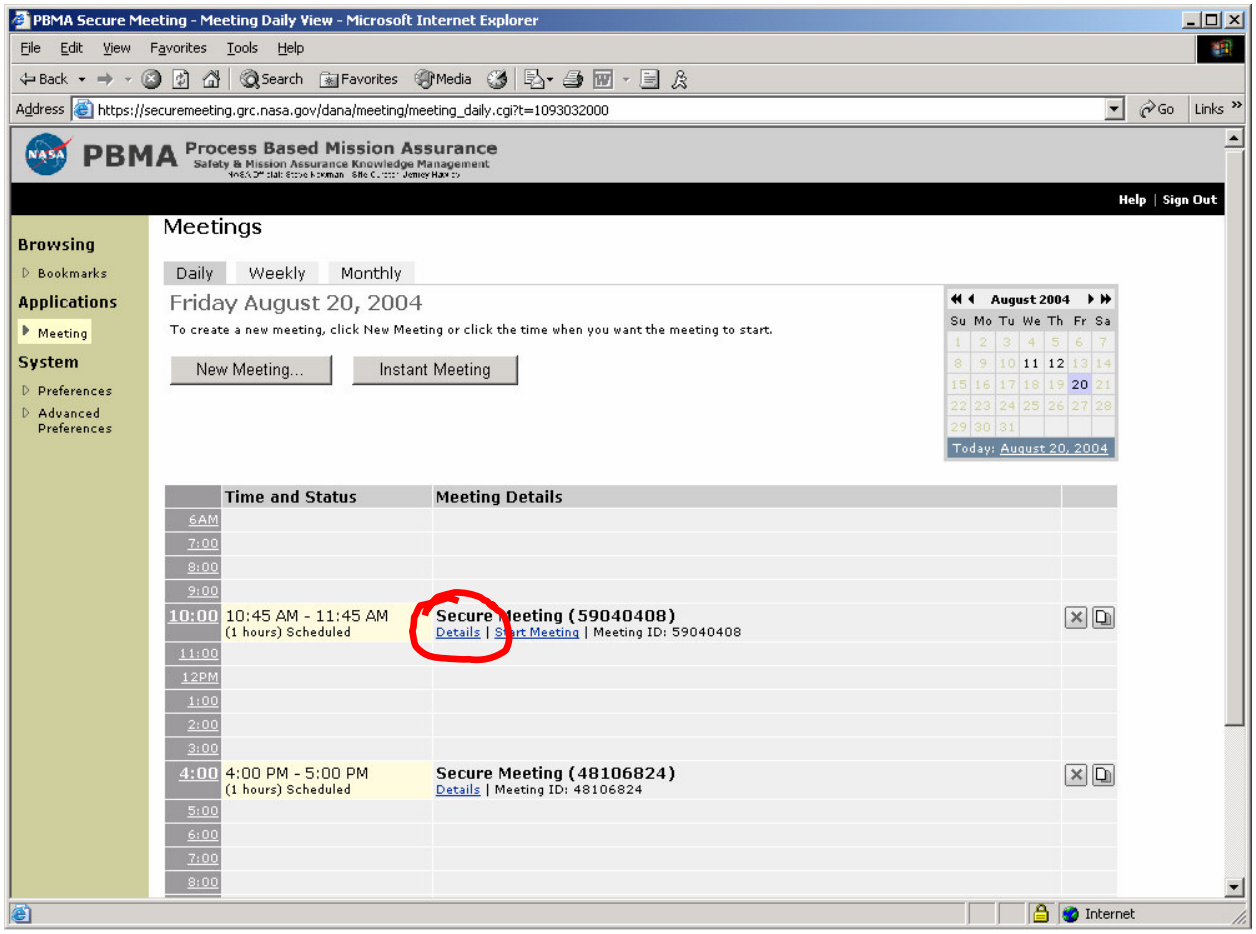
4 Scheduling, Attending, and Running Meetings

4.1 Scheduling Meetings

4.1.1 Creating Meetings

Through the "Meeting" tab, individuals scheduling meetings must specify meeting details, including the type of meeting (New or Instant), meeting name, description, start time, start date, duration, and the list of invitee's usernames.

Meetings Page



SecureMeeting sends an individual notification email to each invitee. Email addresses are obtained from the "Preferences" page as outlined in Section 3, Task 7 of this document. (This email is automatically used when that attendee is invited to a meeting.)

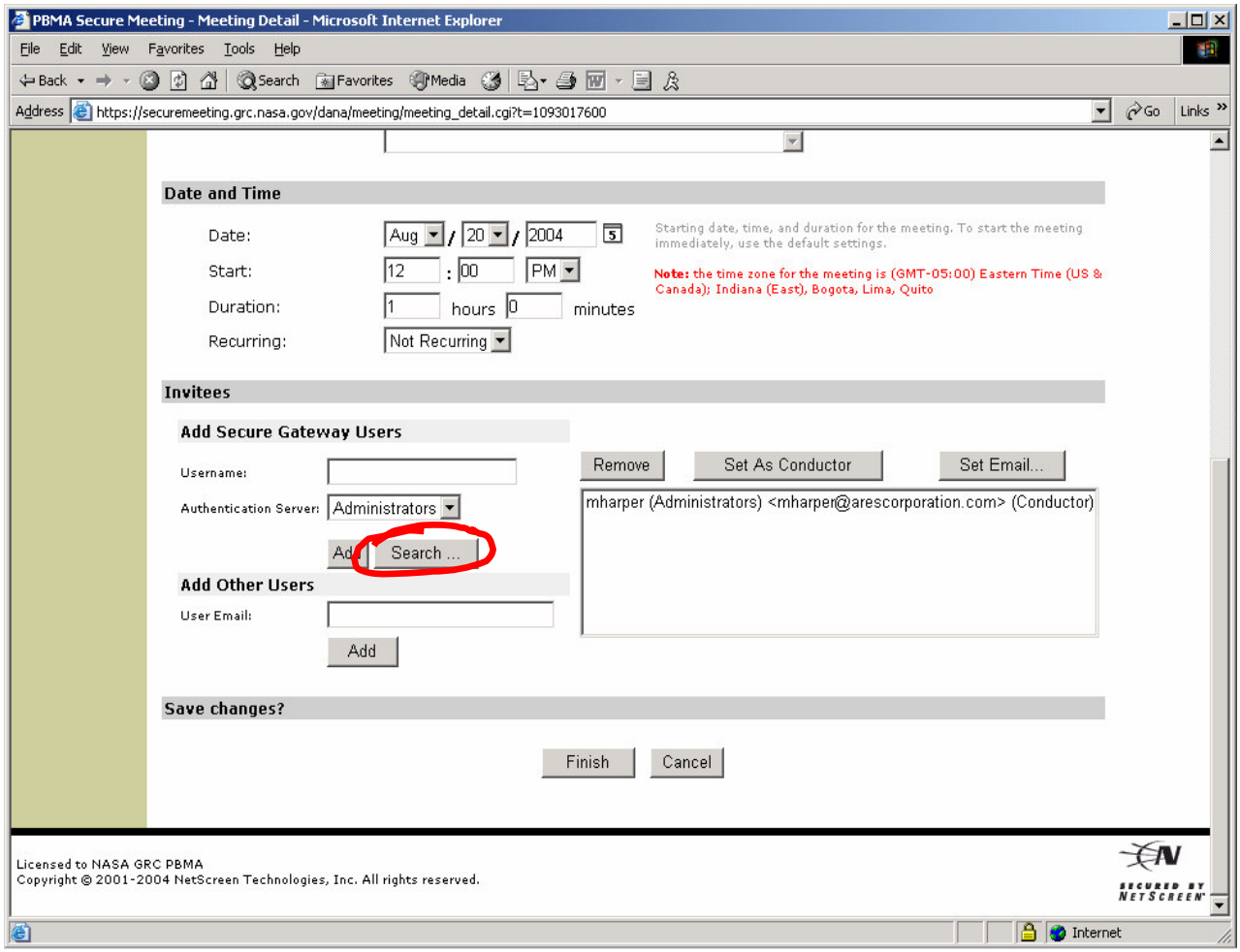
The meeting creator may choose to bypass most meeting scheduling steps and create an Instant Meeting by user clicking the "Instant Meeting" tab. The system automatically generates a meeting with a unique name to start immediately for a specified duration of 30 minutes, adds the meeting creator as the only invitee, and brings up the "Launch Meeting Application" page on the meeting creator's desktop. Once the instant meeting is

launched, the creator may go to the “Meeting” tab on the Meetings Page and add meeting participants through the “Details” button, as seen in the above screenshot.

4.1.2 Meeting Invitees

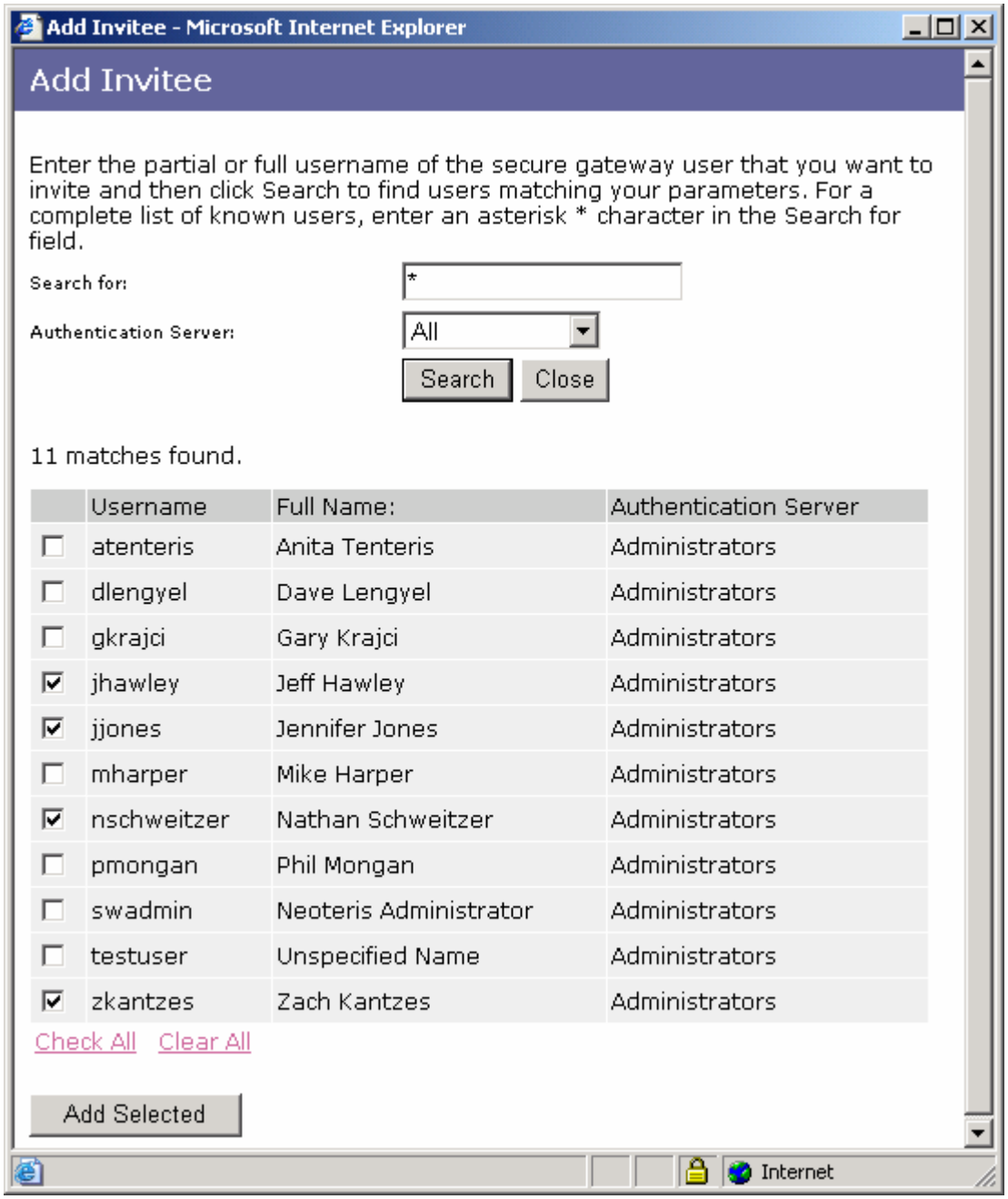
When the meeting creator specifies who they want to invite, the prospective attendee must have a SecureMeeting account. Through the “Details” button on the Meetings page, individuals may be sent invitations to join the meeting.

Meeting Details



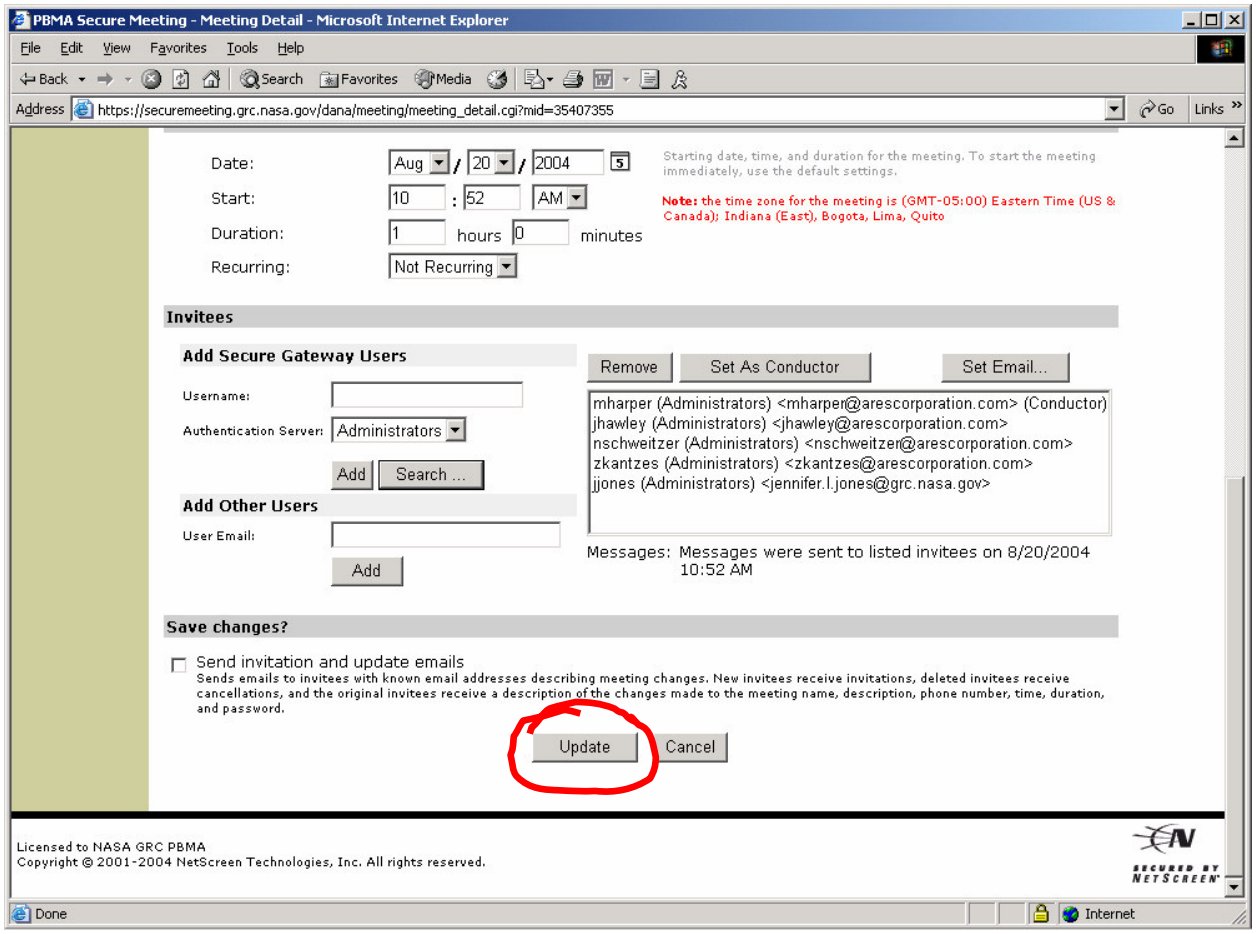
By clicking the “Search” button, you can find the names of the individuals that you want to attend your meeting. Enter the partial or full username of those individuals that you want to invite and then click “Search” to find users matching your parameters. For a complete list of known users, enter an asterisk * character in the Search for field.

Interface for Adding Meeting Invitees



Check the box next to the username of the individual(s) you want to invite and click "Add Selected" to populate the meeting. Once all invitees are set you may send notices under the "Save Changes?" section on the Meeting Details page. If you are initially setting up the meeting, then click "Finish" to complete the meeting and send invitations. If it is an Instant Meeting or you are updating or making changes to an existing meeting click "Update" to complete the meeting and sent invitations.

Meeting Details



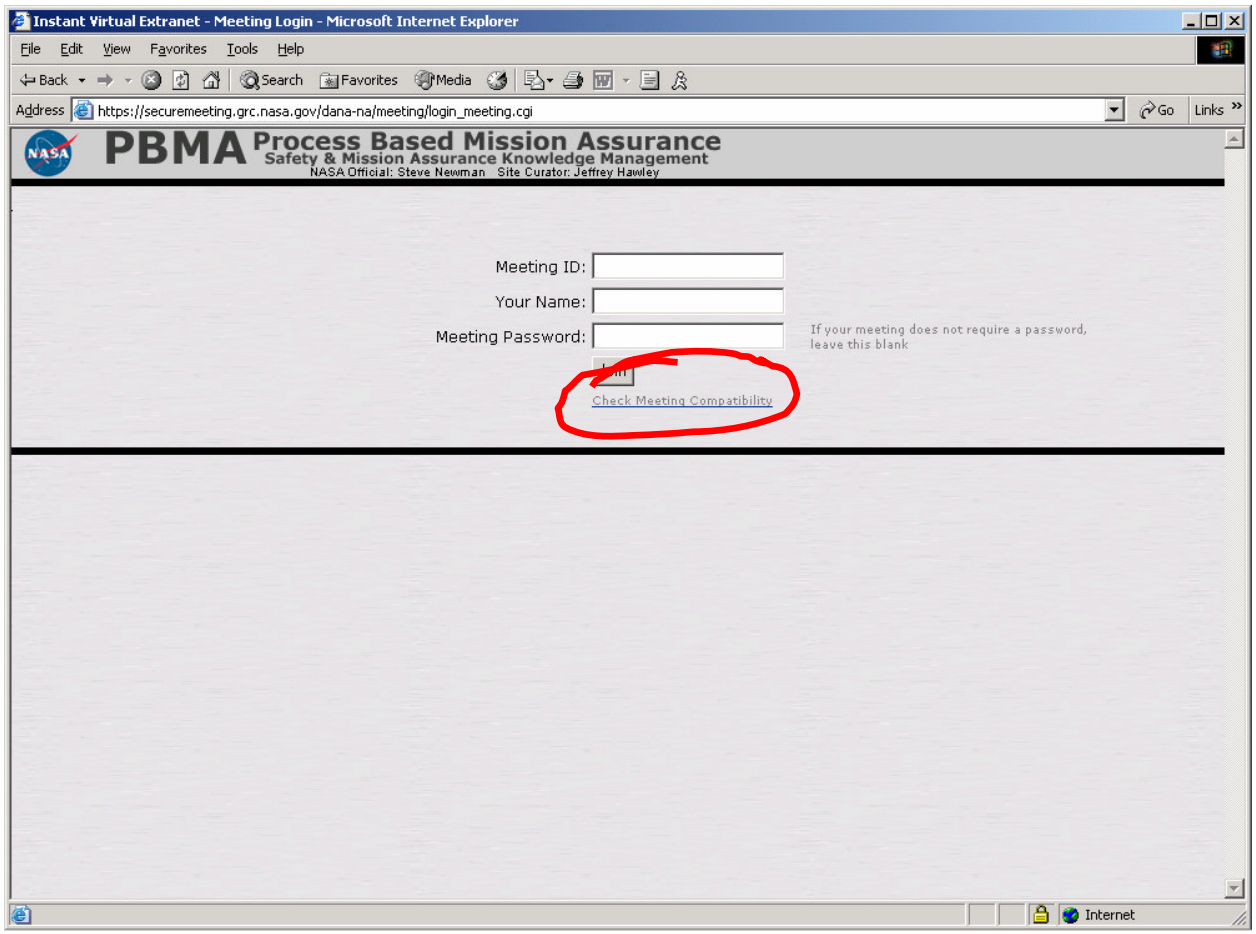
Note: Under the "Invitees" section on the Meeting Details Page, the "Add Other Users" button will send an invitation to any email you add but if that individual does not have a SecureMeeting account they **WILL NOT** be able to join the meeting.

4.2 Attending Meetings

4.2.1 PBMA SecureMeeting Supported Environments

SecureMeeting is designed to work in a variety of environments. Depending on how your system is configured, SecureMeeting may operate slightly different. The easiest way to determine if your system is compatible with SecureMeeting application is to use the SecureMeeting Compatibility Checker. To use this feature, go to the meeting sign-in page using the meeting URL (https://securemeeting.grc.nasa.gov/meeting/) and click "Check Meeting Compatibility".

PBMA SecureMeeting Compatibility Checker



This tool determines your compatibility level and suggests upgrades to achieve full compatibility if required. You may run the compatibility checker at any time after scheduling a meeting - you do not have to wait until the meeting is about to begin.

Note: The SecureMeeting compatibility checker does not check your connection speed or miscellaneous other factors that will not affect your system's compatibility, but may affect your meeting experience.

4.2.1.1 Operating system and browser requirements

PBMA SecureMeeting is supported at different levels on different operating systems. If you run SecureMeeting on a:

- **Windows operating system** - You can access all meeting functionality. Supported Windows operating systems include Windows 98 SE, Windows ME, Windows 2000 with service pack 4, Windows NT 4.0 with service pack 6, and Windows XP with service pack 1. Supported browsers on Windows operating systems include Internet Explorer 6.0 with service pack 1 and Netscape Navigator 7.1. Additionally, Internet Explorer versions 5.0 and 5.5 with service pack 2 are

supported on all of the Windows operating systems listed above except Windows XP.

- **Non-Windows operating system** - SecureMeeting should work on any operating system with the correct Java Virtual Machine (JVM) installed on it, but we recommend MacX 10.3 with Safari 1.1.1 or Linux RedHat 7.3 with Mozilla 1.1 in non-Windows environments. In addition to the browser requirements listed above, you must also enable JavaScript and one of the following components through your browser. If Active-X components are enabled through your browser, SecureMeeting downloads an Active-X component on to your client machine when you join a meeting. Otherwise, if you have a JVM installed, SecureMeeting downloads a Java applet when you join a meeting:
    - **Active X components—**Active-X controls are automatically enabled for administrators and power users on Windows 2000 systems, but standard users must enable them manually. To enable Active-X controls in Internet Explorer*, choose **Tools > Internet Options > Security > Custom Level**, and then enable Active-X components through the **Security Settings** dialog box.
    - **Microsoft Java Virtual Machine (JVM)—**To enable Microsoft JVM in Internet Explorer*, choose **Tools > Internet Options > Security > Custom Level**, and then enable **Microsoft VM** through the **Security Settings** dialog box.
    - **Sun Java Virtual Machine (JVM) 1.4 .1_01 or above—**SecureMeeting runs a Java applet in memory on your machine when you join a meeting. SecureMeeting is supported with Sun JVMs versions 1.4.1_01 and above. You can download the Sun JVM from www.java.com.

  To enable JavaScript through:
    - **Internet Explorer***—Navigate to **Tools > Internet Options > Security** tab, and choose **Custom Level**. Under **Scripting of Java applets**, choose **Enable**.
    - **Netscape Navigator***—Navigate to **Edit > Preferences**. Under **Advanced > Scripts & Plugins**, select the **Navigator** check box.

4.2.1.2 Additional requirements and restrictions

PBMA SecureMeeting supports running meetings with monitor displays up to 32-bit color. PBMA SecureMeeting cannot be used to share streaming media applications.

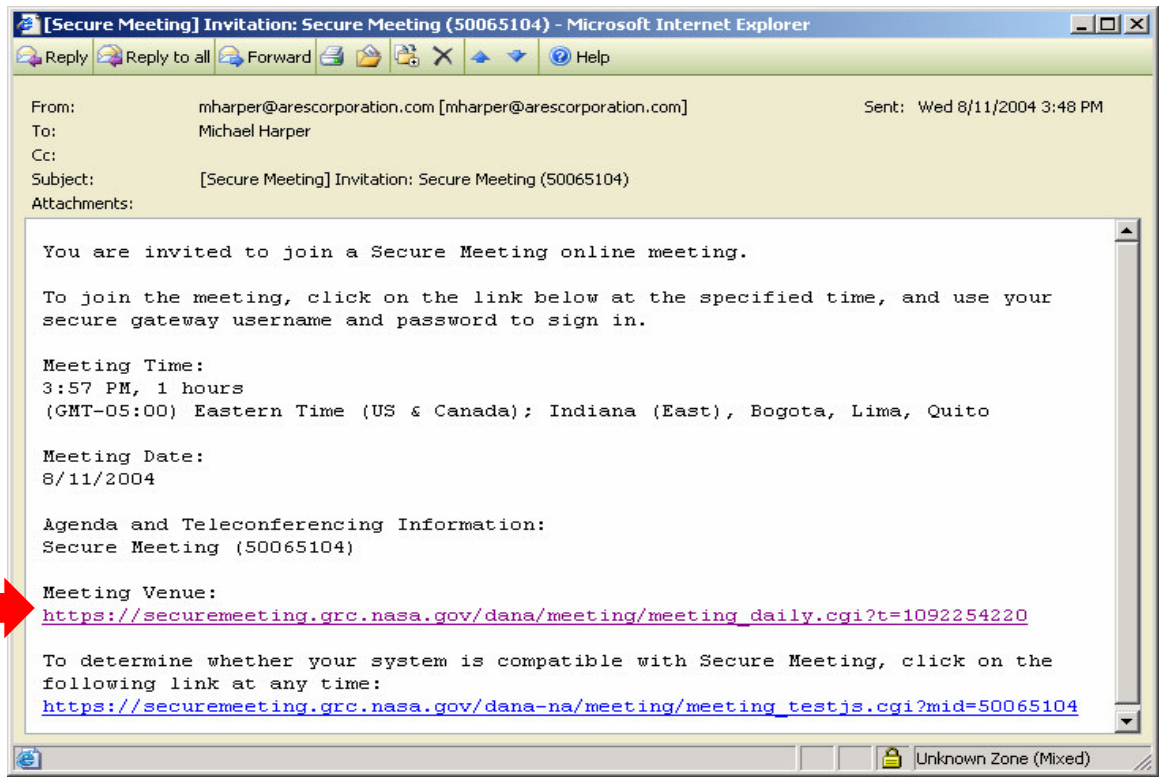
4.2.2 Accessing the Meeting URL

To attend a meeting, PBMA SecureMeeting invitees must navigate to the meeting site using their SecureMeeting Account. The following steps outline the way in which a SecureMeeting invitee receives notification of a meeting.

* The instructions shown here are for the latest browser versions. Instructions may vary for older browsers.

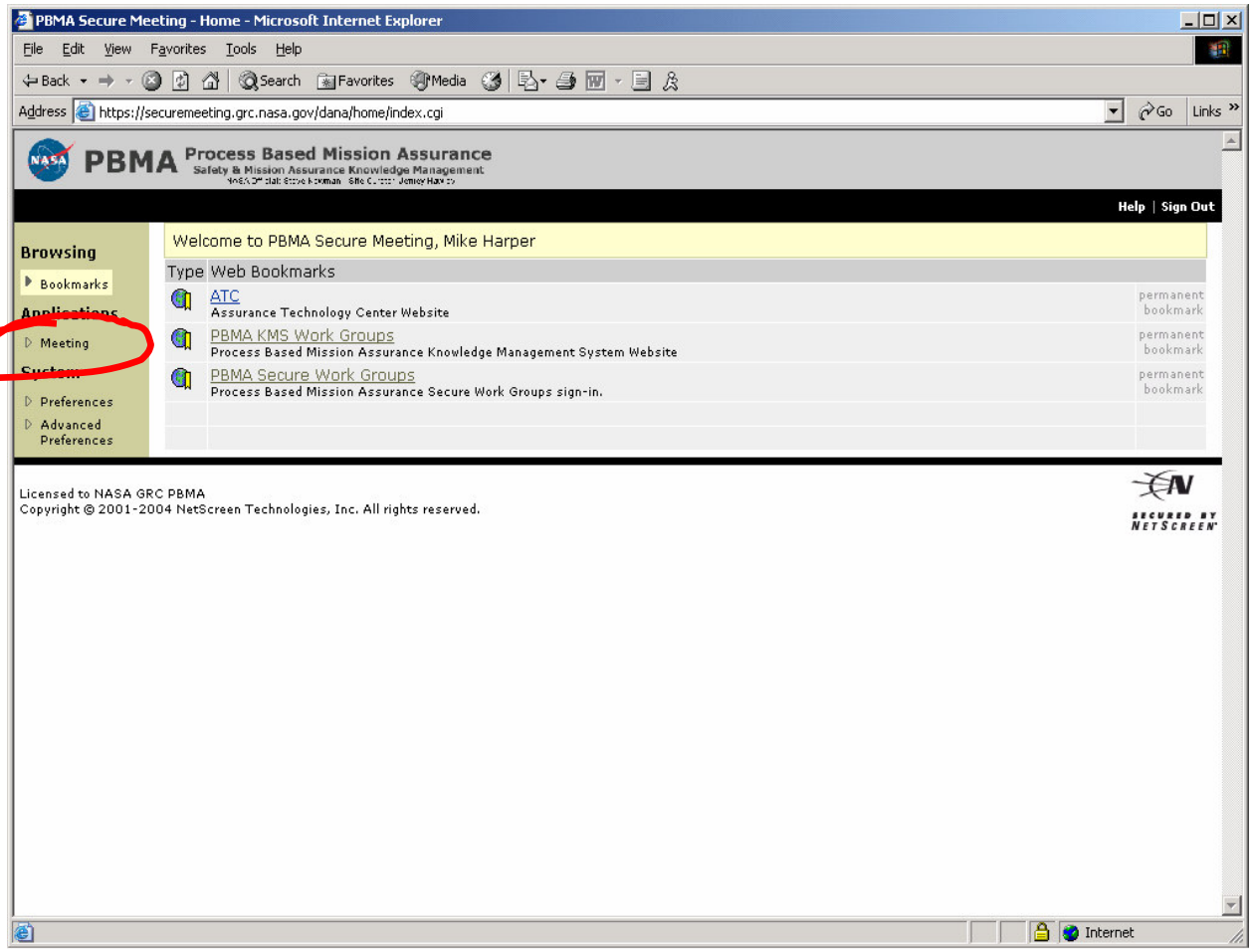
1. The invitee will receive an email that will contain the meeting time, duration, date, agenda, teleconference information, meeting venue URL, and system compatibility checker URL.
2. Click in the URL under the "Meeting Venue" provided in the SecureMeeting notification email and you will receive the SecureMeeting login page.

SecureMeeting Notification Email



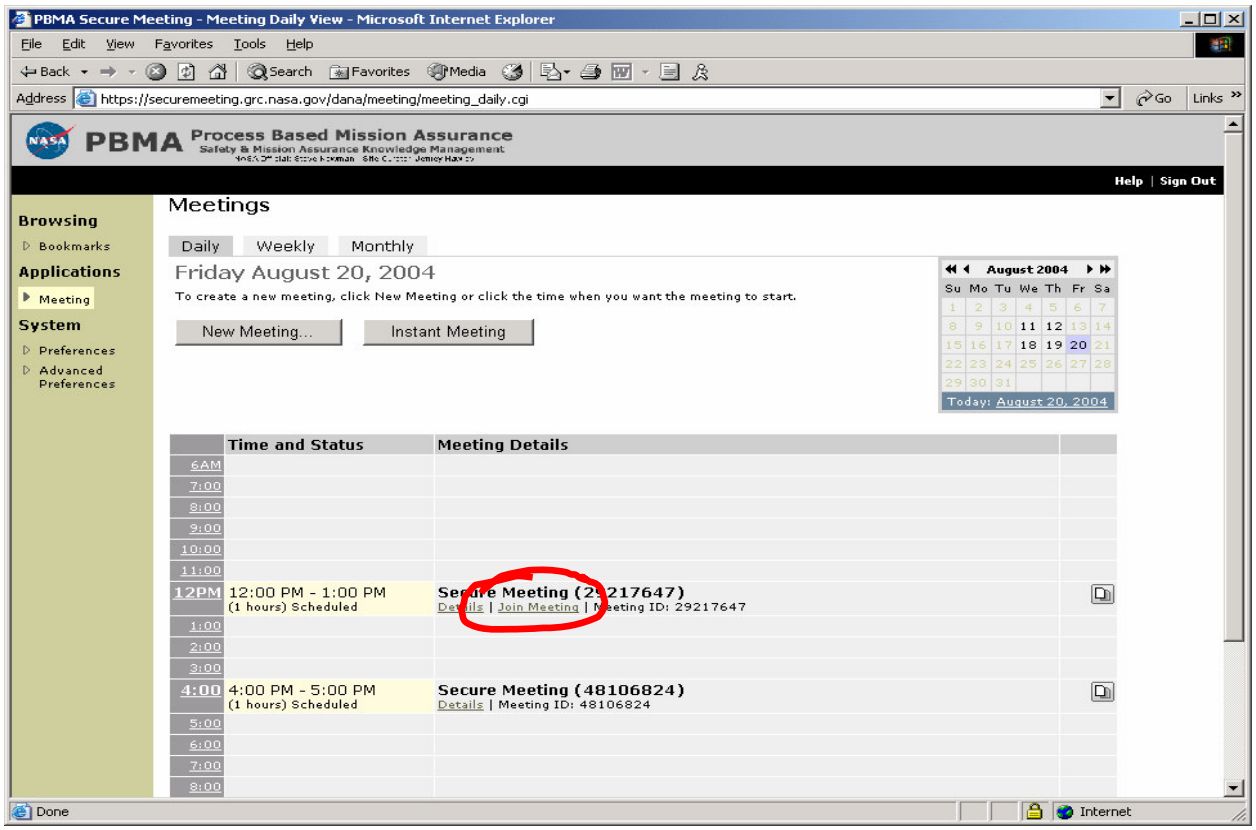
3. Click the "Meeting" link provided on the SecureMeeting Welcome Page.

SecureMeeting Welcome Page



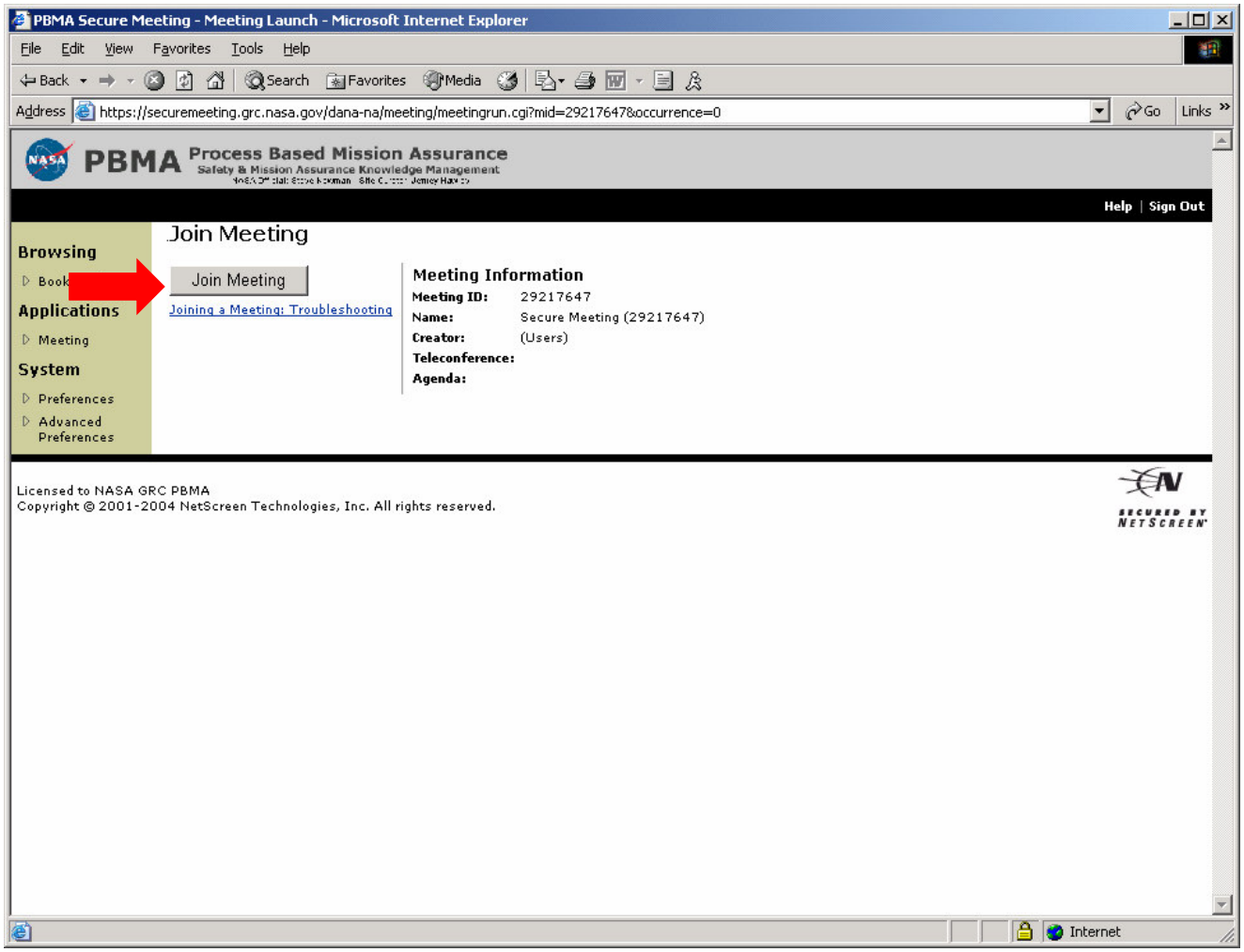
4. The link will take you to the SecureMeeting Calendar where you can view all meetings in which you have either as scheduled or been invited to participate.

SecureMeeting Calendar



5. The meeting that you are to join will be in your calendar, click the "Join Meeting" link to take you to the "Join Meeting" Interface.

"Join Meeting" Interface



4.2.3 Joining the Meeting

When the invitee chooses to join a meeting, the PBMA SecureMeeting application downloads either an Active-X component or a Java applet on to the invitee's system. Again, if Active-X components are enabled through your browser, SecureMeeting downloads an Active-X component on to your client machine when you join a meeting. Otherwise, if you have a JVM installed, SecureMeeting downloads a Java applet when you join a meeting. This client-side component contains:

- a meeting viewer
- presentation tools
- a text messaging application

Once PBMA SecureMeeting launches the Active-X or Java applet on the user's desktop, the user becomes a meeting attendee and can begin participating in the meeting. Attendees are allowed to join up to 15 minutes before the meeting is scheduled to start.

Macintosh users may be asked to accept two certificates:

1. "Thawte Consulting cc" (SSL certificate)
2. "Sun Microsystems" (JVM applet)

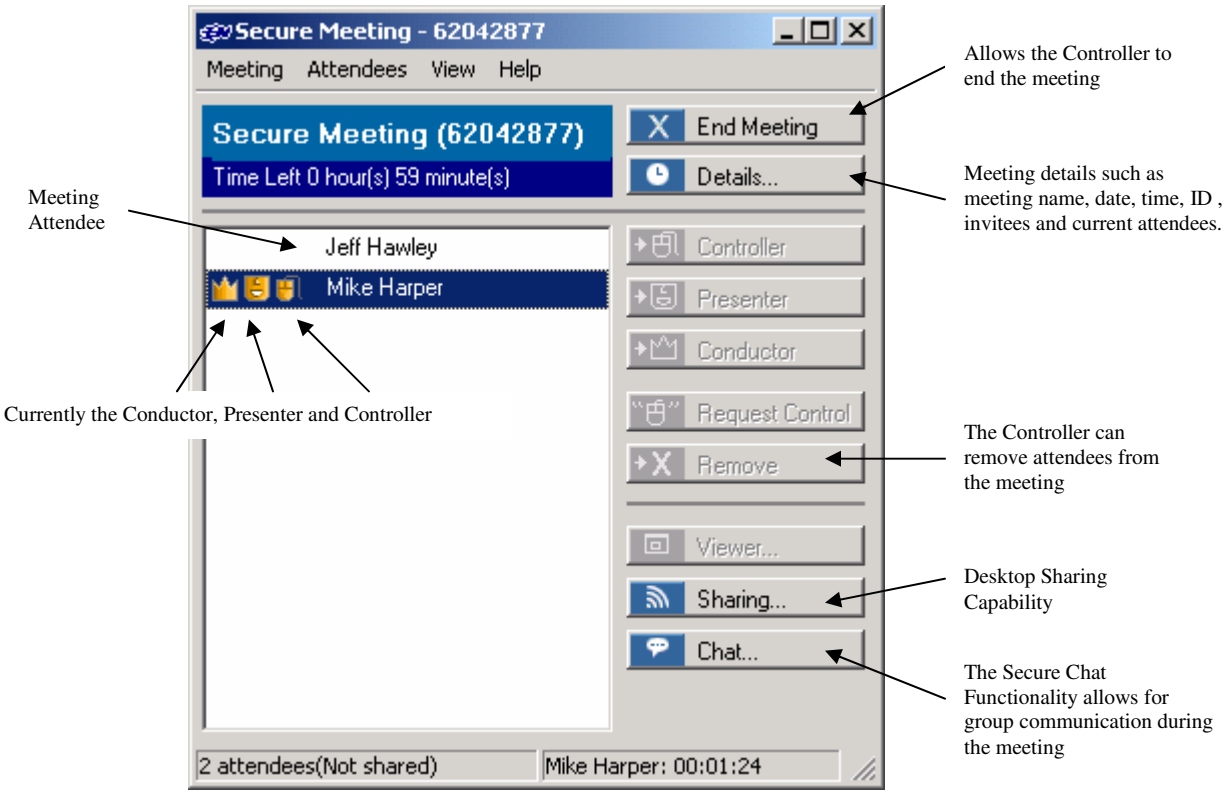
You must accept both of these certificates to launch SecureMeeting.

4.3 Running meetings

4.3.1 Meeting Viewer

Once the meeting scheduler or invitee clicks the "Start Meeting" or "Join Meeting" button the Meeting Viewer will be launched:

Meeting Viewer



4.3.2 Meeting Roles and Functionality

The individual who scheduled the meeting is also the default ***Meeting Conductor*** ("Conductor") within the SecureMeeting application. The Conductor is responsible for starting the meeting, ending the meeting and assigning the Presenter role. Before the Conductor joins, the other attendees can only chat. They cannot view or make a presentation because the Conductor is also the default ***Meeting Presenter*** ("Presenter"). The Conductor (or a meeting attendee that is designated as a Presenter) starts the meeting presentation by sharing his desktop or applications with other attendees. Once the

Presenter begins sharing, a meeting viewer automatically opens on all of the meeting attendees' desktops and displays the presenter's shared application[*].

The Conductor is also responsible for expelling meeting attendees if necessary, extending the meeting if it runs over the scheduled duration, and closing the meeting when it is done. The meeting Conductor may pass his responsibilities to another attendee during the meeting provided the selected attendee is running in the correct environment. The Conductor may designate any other SecureMeeting account owner as a Conductor and any other Windows user attendee as a Presenter.

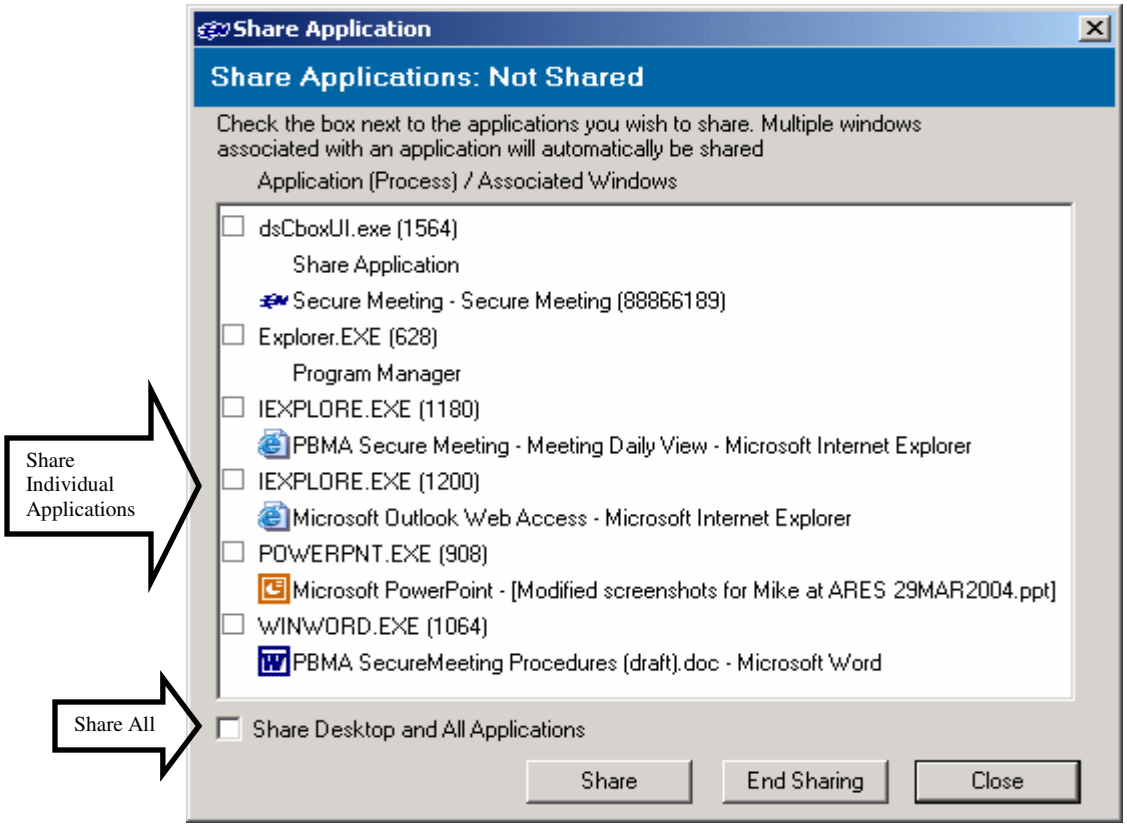
The Presenter may also pass responsibilities to another attendee by designating a ***Controller***. A Controller uses his own mouse and keyboard to remote control the Presenter's shared desktop or applications. Note that the Presenter can pass remote control rights to any other attendee - he is not restricted to Windows user attendees. When the Presenter wants to regain control of his remote-controlled applications, he simply needs to right-click anywhere and SecureMeeting returns control to the Presenter.

4.3.3 Desktop Sharing

As previously mentioned, the Presenter starts the meeting presentation by sharing his desktop or applications with other attendees. Once the Presenter begins sharing, a meeting viewer automatically opens on all of the meeting attendees' desktops and displays the presenter's shared application. The Desktop Sharing Capability can be accessed through the "Sharing" button. The Presenter can select to share individual applications on their desktop or can share the entire desktop as seen below.

[*] SecureMeeting cannot display the content of a meeting presenter's desktop if it is locked.

Sharing Interface (PC only)

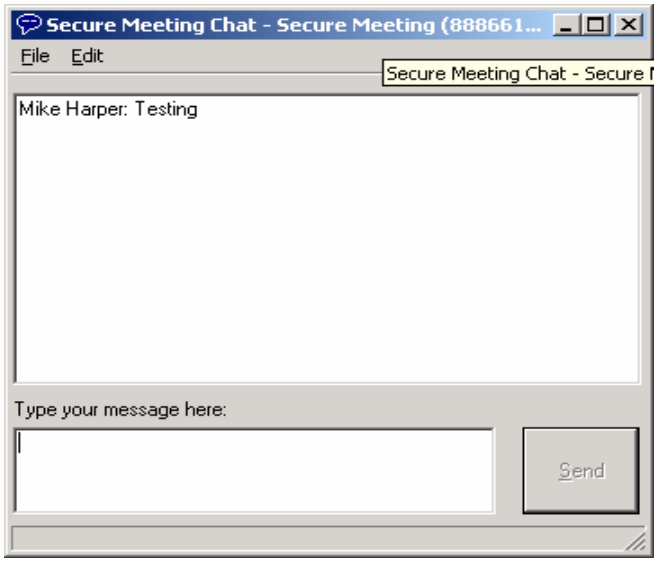


Note: Macintosh users will not have the option of itemizing what they share - it is set up to share all or nothing in the Macintosh environment.

4.3.4 Secure Chat Functionality

The SecureMeeting Chat Functionality allows for group communication during the meeting and all attendees can access the chat feature. As soon as an attendee joins a meeting, they may start sending text messages to one other using the "SecureMeeting Chat" window, even if the Controller has not yet joined.

SecureMeeting Chat Window



5 Getting Help

PBMA Technical Support is available if you encounter any problems with the PBMA SecureMeeting system. Technical Support can be contacted via email at pbma.admin@arescorporation.com. All issues sent to Technical Support pertaining to the SecureMeeting application should have "PBMA SecureMeeting" in the subject line.

The following information must be in the email to PBMA Technical Support:

- Name
- Work Phone
- SecureMeeting User ID
- Description of the Problem or Request

In addition to the information identified above, please have the following available if Technical Support should need to contact you by telephone:

- Steps to re-create problem, if known
- System information
  - Browser - Application (Internet Explorer or Netscape) and version
  - Operating System - Application (Windows or Mac) and version
- Access location
  - Center/facility or organization

Standard operating hours of Technical Support are Monday through Friday 8:00 AM to 5:00 PM Eastern. Technical Support will observe all NASA holidays. Any requests received outside of standard operating hours will be handled as soon as possible the following business day.